For this programming assignment we were tasked with writing a firewall with the specific rules from the assignment steps.

1. Flush and delete all previously defined rules and chains

2. Write a rule that only accepts packets that originate from f1.com.

3. For all outgoing packets, change their source IP address to your own machine’s IP address (Hint: Refer to the MASQUERADE target in the nat table).

4. Write a rule to protect yourself against indiscriminate and nonstop scanning of ports on your machine.

5. Write a rule to protect yourself from a SYN-flood Attack by limiting the number of incoming ’new connection’ requests to 1 per second once your machine has reached 500 requests. 2

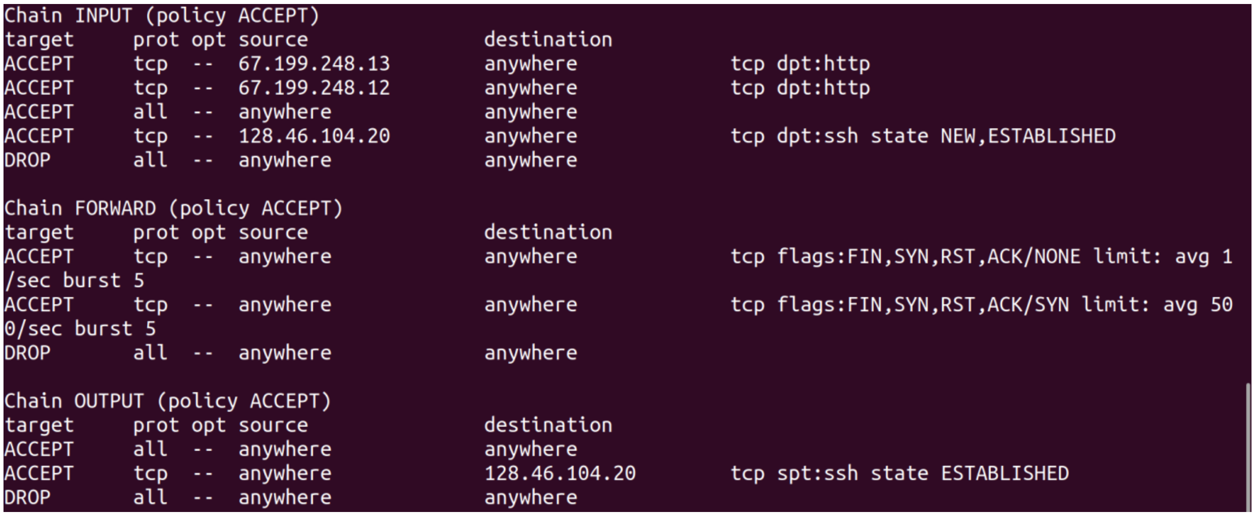
6. Write a rule to allow full loopback access on your machine i.e. access using localhost (

7. Write a port forwarding rule that routes all traffic arriving on port 8888 to port 25565

8. Write a rule that only allows outgoing ssh connections to engineering.purdue.edu.

9. Drop any other packets if they are not caught by the above rules.

We then get the firewall output from f1.com as such:

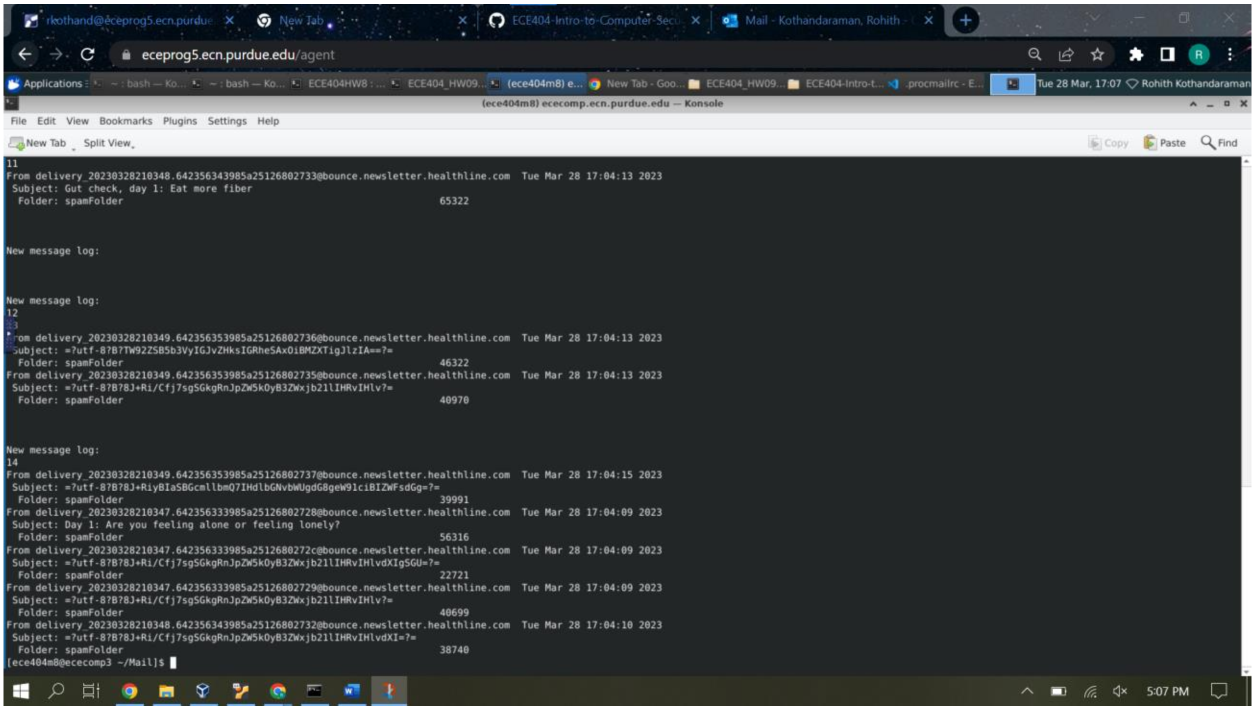


```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  67.199.248.13        anywhere             tcp dpt:http
ACCEPT     tcp  --  67.199.248.12        anywhere             tcp dpt:http
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  128.46.104.20        anywhere             tcp dpt:ssh state NEW,ESTABLISHED
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/NONE limit: avg 1
/sec burst 5
ACCEPT     tcp  --  anywhere             anywhere             tcp flags:FIN,SYN,RST,ACK/SYN limit: avg 50
0/sec burst 5
DROP       all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
ACCEPT     tcp  --  anywhere             128.46.104.20        tcp spt:ssh state ESTABLISHED
DROP       all  --  anywhere             anywhere
```

In this step we setup a spam filter and we test it by subscribing to several newsletters for spam



```
11
From delivery_20230328210348.642356343985a25126802733@bounce.newsletter.healthline.com  Tue Mar 28 17:04:13 2023
 Subject: Gut check, day 1: Eat more fiber
  Folder: spamFolder                                                    65322



New message log:



New message log:
12
13
From delivery_20230328210349.642356353985a25126802736@bounce.newsletter.healthline.com  Tue Mar 28 17:04:13 2023
 Subject: =?utf-8?B?TW92ZSB5b3VyIGJvZHksIGRheSAxOiBMZXTigJlzIA==?=
  Folder: spamFolder                                                    46322
From delivery_20230328210349.642356353985a25126802735@bounce.newsletter.healthline.com  Tue Mar 28 17:04:13 2023
 Subject: =?utf-8?B?8J+Ri/Cfj7sgSGkgRnJpZW5kOyB3ZWxjb21lIHRvIHlv?=
  Folder: spamFolder                                                    40970



New message log:
14
From delivery_20230328210349.642356353985a25126802737@bounce.newsletter.healthline.com  Tue Mar 28 17:04:15 2023
 Subject: =?utf-8?B?8J+RiyBIaSBGcmllbmQ7IHdlbGNvbWUgdG8geW91ciBIZWFsdGg=?=
  Folder: spamFolder                                                    39991
From delivery_20230328210347.642356333985a25126802728@bounce.newsletter.healthline.com  Tue Mar 28 17:04:09 2023
 Subject: Day 1: Are you feeling alone or feeling lonely?
  Folder: spamFolder                                                    56316
From delivery_20230328210347.642356333985a2512680272c@bounce.newsletter.healthline.com  Tue Mar 28 17:04:09 2023
 Subject: =?utf-8?B?8J+Ri/Cfj7sgSGkgRnJpZW5kOyB3ZWxjb21lIHRvIHlvdXIgSGU=?=
  Folder: spamFolder                                                    22721
From delivery_20230328210347.642356333985a25126802729@bounce.newsletter.healthline.com  Tue Mar 28 17:04:09 2023
 Subject: =?utf-8?B?8J+Ri/Cfj7sgSGkgRnJpZW5kOyB3ZWxjb21lIHRvIHlv?=
  Folder: spamFolder                                                    40699
From delivery_20230328210348.642356343985a25126802732@bounce.newsletter.healthline.com  Tue Mar 28 17:04:10 2023
 Subject: =?utf-8?B?8J+Ri/Cfj7sgSGkgRnJpZW5kOyB3ZWxjb21lIHRvIHlvdXI=?=
  Folder: spamFolder                                                    38740
[ece404m8@ececomp3 ~/Mail]$ 
```